

REMARKS

Claims 1-9, 11-16, 25-31, and 33-36 remain pending in the application. Claims 1, 3-4, 8-9, 11-12, 25, and 31 have been amended to clarify claimed subject matter and/or correct informalities. Support for the claim amendments may be found in the original specification at least at pages 4, 12, 14, 24, 25 and at least in Figures 1, 2, 3, and 9. No new matter has been introduced by these amendments.

Claims 1-9, 11-16, 25-31, and 33-36 are for consideration upon entry of the present Amendment. Applicant requests favorable reconsideration of this response and allowance of the subject application based on the following remarks.

Claim Rejections under 35 U.S.C. § 103

Claims 1-9, 11-16, 25-31, and 33-36 stand rejected under 35 U.S.C. §103(a) for obviousness over U.S. Patent No. 6,829,357 to Alrabady et al. (hereinafter "Alrabady") in view of U.S. Patent No. 6,804,355 to Graunke (hereinafter "Graunke"). Applicant respectfully traverses the rejection. To establish a *prima facie case* of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations (see, MPEP 2142).

Without conceding the propriety of the stated rejections, and only to advance the prosecution of this application, Applicant has amended **independent Claim 1**, to clarify further features of the subject matter.

Independent Claim 1 recites a computer readable media including:

receiving requirements to protect an original digital good;
parsing the original digital good along natural boundaries into
portions;
selecting a first portion of the original digital good;
generating a substitution box (S-box) that includes a byte or bit
values from the first portion of the original digital good;
identifying a second portion of the original digital good, wherein
the second portion is to be encrypted;
mapping the byte or bit values of the second portion to
substitution byte or bit values based on the substitution box (S-box)
when encrypting the second portion; and
outputting a protected digital good that is functionally equivalent
to and derived from the original digital good.

References Do Not Teach or Suggest Parsing, Generating S-box, Mapping, Outputting:

Alrabady is directed to size reduction for encrypted data communication signals of a remote convenience system (col. 1, lines 8-10). The portions of the message information that are encrypted preferably include the security code, the command(s), and a sequence counter to further increase security (col. 4, lines 1-5). Thus, Applicant asserts Alrabady fails to disclose, teach or suggest “parsing the original digital good along natural boundaries into portions; generating a substitution box (S-box); mapping the byte or bit values; and outputting a protected digital good that is functionally equivalent to and derived from the original digital good”, as recited in Claim 1.

Graunke does not compensate for the deficiencies of Alrabady. Graunke constructs S-boxes by a message digest function used as a pseudo-random number generator and one of a plurality of keys (col. 1, lines 45-47). In Graunke, a permutation of integers may be computed using the message digest as a cryptographic strength pseudo-random number generator and keys (col. 2, lines 58-62). Furthermore, the substitution

effects are generated by message digests with restricted inputs and truncated outputs (col. 2, lines 37-38). Thus, even if, for the sake of argument, the teachings of Graunke can be used to modify Alrabady, the combination would still lack at least “parsing the original digital good along natural boundaries; generating a substitution box that includes a byte or bit values from the first portion of the original digital good; and mapping the byte or bit values of the second portion to substitution byte or bit values based on the substitution box to encrypt the second portion”, as recited in Claim 1.

Applicant asserts the Office has not provided sufficient evidence that Alrabady or Graunke, alone or in combination, discloses, teaches, or suggests the features of Claim 1, as shown above.

Furthermore, the Office has failed to establish a motivation sufficient for one of ordinary skill in the art to combine the references. The motivation provided by the Office “for the advantage of the resistance to differential and linear cryptanalysis that S-boxes bring” is very general because it could cover almost any alteration contemplated of Alrabady. A sequence counter is used in Alrabady to increase security as part of the encryption for each transmission (col. 1, line 52), so S-boxes are not advantageous for Alrabady to resist cryptanalysis. This rejection is improper.

In addition, there is no teaching or suggestion to implement a key as an S-box taught by Graunke using one portion of message as a key to encrypt and decrypt another portion of message taught by Alrabady. The Office cannot improperly rely on hindsight by locating references without evidence of motivation to propose the suggested combination.

Independent Claim 8 recites features similar to those of Claim 1 discussed above and is, therefore, allowable for at least substantially the same reasons as Claim 1.

Dependent Claims 2-7, 9, and 11-16 depend from one of Claims 1 and 8 and are allowable by virtue of this dependency, as well as for the additional features that they recite. Applicant respectfully requests that the §103 rejection be withdrawn.

References Do Not Teach or Suggest An Analyzer, Production Server

Turning now to **Independent Claim 25**, which is amended to clarify further features of the subject matter, recites:

A production system, comprising:

a memory to store an original digital good, wherein the original digital good is transformed into a protected digital good;

an analyzer to parse the original digital good along natural boundaries into segments; and

a production server equipped with a substitution box (S-box) protection tool that is used to augment the original digital good for protection purposes, the production server being configured to identify a first segment in the original digital good and use a byte or bit values from the first segment in an S-box when encrypting a second segment of the original digital good.

Alrabady and Graunke alone or in combination, do not teach or suggest “an analyzer to parse the original digital good along natural boundaries into segments; the production server being configured to identify a first segment in the original digital good and use a byte or bit values from the first segment in an S-box when encrypting a second segment of the original digital good”, as recited in Claim 25. This claim is amended along the same lines as Claim 1, and hence benefits from the same arguments. Therefore, this claim is allowable.

Dependent Claims 26-30 are allowable by virtue of their dependency from Claim 25, respectively, as well as for the additional features that they recite. Applicant respectfully requests that the §103 rejection be withdrawn.

References Do Not Teach or Suggest An Analyzer, Production Server, Digital Good Functionally Equivalent to and Derived from Original Digital Good

Turning now to **Independent Claim 31**, which is amended to clarify further features of the subject matter, recites:

A client-server system, comprising:
a production server to receive requirements to protect an original digital good;
an analyzer in the production server to parse the digital good along natural boundaries into portions;
the production server to use a byte or bit value from a portion of a first digital good in a substitution box (S-box) to encrypt at least a portion of a second digital good to produce a protected digital good;
a client to store and execute the protected digital good, the client being configured to evaluate the protected digital good to determine whether the protected digital good has been tampered with;
wherein the first digital good and the second digital good are the same digital good; and
wherein the protected digital good is functionally equivalent to and derived from the original digital good.

Alrabady and Graunke alone or in combination, do not teach or suggest “an analyzer in the production server to parse the original digital good along natural boundaries into portions; the client being configured to evaluate the protected digital good to determine whether the protected digital good has been tampered with; wherein the protected digital good is functionally equivalent to and derived from the original digital good”, as recited in Claim 31. This claim is amended along the same lines as Claim 1, and hence benefits from the same arguments. Therefore, this claim is allowable.

Dependent Claims 33-36 are allowable by virtue of their dependency from Claim 31, respectively, as well as for the additional features that they recite. Applicant respectfully requests that the §103 rejection be withdrawn.

Conclusion

Claims 1-9, 11-16, 25-31, and 33-36 are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Office is requested to contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Dated: Dec. 29, 2006

By: Shirley Lee Anderson
Shirley Lee Anderson
Reg. No. 57,763
(509) 324-9256 ext. 258